PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/JP2004/005528	14.04.2004	24.04.2003

International Patent Classification (IPC) or both national classification and IPC
H04L9/30

Applicant
MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☒ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Bec, T

Telephone No. +49 89 2399-7124

ATTACHMENT G

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/JP2004/005528

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was field, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. II Priority

1. ☒ The following document has not been furnished:

   ☒ copy of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(a)).

   ☐ translation of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(b)).

   Consequently it has not been possible to consider the validity of the priority claim. This opinion has nevertheless been established on the assumption that the relevant date is the claimed priority date.

2. ☐ This opinion has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rules 43*bis*.1 and 64.1). Thus for the purposes of this opinion, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-37
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-37
Industrial applicability (IA)	Yes:	Claims	1-37
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item I.

1 The following document is referred to in this communication:
D1 : J. SILVERMAN: "WRAPS, GAPS, AND LATTICE CONSTANTS" NTRU CRYPTOSYSTEMS TECHNICAL REPORT, REPORT 11, [Online] 15 March 2001 (2001-03-15), pages 1-6, XP002288211 Retrieved from the Internet: URL:http://www.ntru.com/cryptolab/pdf/NTRU Tech011_v2.pdf>; [retrieved on 2004-07-12]

Re Item V.

1) The present set of claims lacks of conciseness as it contains 21 independent claims with overlapping scope within the following groups of claims:

i) encryption system and apparatus 18, 20, 21, 22, 23, 30, 31 and 32,
ii) decryption system and apparatus 19, 26, 27 and 35,
iii) encryption method 24 and 33,
iv) decryption method 28 and 36,
v) encryption program 25 and 34,
vi) decryption program 29 and 37,

thus the application does not comply with the provision of clarity and conciseness Article 6 PCT.

2) None of the independent claims meets the requirements of Article 6 PCT as they define the subject-matter in terms of the result to be achieved without providing technical features to achieve said result:
"a parameter generating apparatus or method which has the property that it cause no decryption error for the NTRU".

3 For the above stated reasons, no examination as to the novelty can be carried out at this stage of the procedure.

4 The present set of claims does not meet the requirements of Article 33(1) and (3) PCT with regard to the inventive step because:
Document D1 cited by the applicant discloses that if all the coefficient of the polynomial "$b=p\phi g + mf$" (see pages 1 and 2) fall in the range [-q/2, q/2] no

decryption error occurs.
In order to have a NTRU system without decryption error, the skilled person will without inventive step add to the generator of polynomials a test to verify the above stated condition before using the polynomials.
Consequently the claimed subject-matter is not inventive.